VPN IS SECURE THEN OTHER PROXIES FOR INTERNET FILTARATION

Nand Kumar Singh [1] | Sunil Kumar Rawani [2] | Hari Shankar Prasad Tonde [2] | Braj Kishor Pathak [2]

[1] Asst. Professor, Computer Sc. & Application, Loyola College Kunkuri , Dist.-Jashpur (C.G.), India -496225.

[2] Research Scholar, Computer Scence, St. Gahira Guru vishwavidyalaya ,Ambikapur (C.G.), India-497001

ABSTRACT

The purpose of using both VPN and proxy servers is to conceal the users identity, or to spoof a certain geo-location (so for example geo-locked services such as many TV streaming websites may be watched outside their country of origin). Many VPN Providers, in addition to offering VPN also provide some kind of proxy service, and there are also many public proxy servers which can be used for free. So the question is 'what is the difference between a proxy and a VPN?'

Although performing a similar function, the actual processes involved are very different, and therefore have very different consequences. The subject is further complicated by the fact that there are a number of different types of proxy services available.

KEYWORDS: VPN, Proxy, Internet.

1. PROXY:

A proxy (technically an open proxy) server is a computer that acts as an intermediary between your computer and the internet. Any traffic routed through a proxy server will appear to come from its IP address, not your computer's. Proxy servers usually communicate with the internet using one of 2 different protocols; HTTP or SOCKS.

HTTP Proxy Servers;

The HTTP protocol is designed to interpret traffic at the HTTP level, which means that it can only handle traffic that starts with http:// or https://, i.e. web pages*. It is therefore only good for web surfing, but because all it is doing is handling HTTP requests, it is faster than either Socks proxies or VPN servers.

Pros:

- Cheap (and often free)
- Will hide your IP from basic checks, and is therefore ok for accessing some geo-restricted websites and for account creation

Cons:

- Only useful for accessing websites*
- Clever use of Flash or JavaScript allows many websites to detect your true IP
- HTTP traffic is not encrypted, so government surveillance systems and your ISP can see what you are doing. If connected through HTTPS (SSL) then traffic cannot be monitored, but the IP of the HTTPS website can be logged. SSL encryption is roughly equivalent to 128-bit key length.
- Each web browser must be configured individually to use the proxy server. However, the good news is that this is well supported by all browsers

SOCKS Proxy Servers:

SOCKS servers do not interpret network traffic at all, which makes them much more flexible, but because they are usually handling more traffic, usually slower. The big advantage of the SOCKS protocol is that it supports any kind of internet traffic, such as POP3 and SMTP for emails, IRC chat, FTP for uploading files to websites, and torrent files. The latest iteration of the protocol is SOCKS5.

Pros:

- Can handle any kind of internet traffic (including torrents)

Cons:

- Slower than HTTP
- Each piece of software (e.g Bit Torrent client) must be configured individually
- Same security issues as HTTP

1.1 Compatibility Issues with Web Proxies:

Web proxies only work for Web traffic, so they cannot be used for other Internet services such as e-mail or instant messaging. Many are also incompatible with complex Web sites like Facebook, streaming multimedia content on sites such as YouTube, and encrypted sites that are accessed through HTTPS. This latter restriction means that many Web proxies will be unable to help you reach filtered sites that require a login, such as Web-based e-mail services. Worse yet, some Web proxies cannot themselves be accessed through HTTPS. If you use such a proxy to log in to a destination site that is normally secure, you may be putting your sensitive information, including your password, at risk. Security issues like this are discussed in more detail below.

With the notable exception of the HTTPS concerns described above, most Web proxy compatibility issues can be resolved by using the "mobile" or "basic HTML" version of the destination Web site, provided one is available. Unfortunately, relatively few sites offer this kind of simplified interface, and even fewer do so in a way that exposes all of the site's functionality. If a Web site does provide a mobile version, its URL will frequently begin with an "m" instead of "www." Examples include https://m.facebook.com, http://m.gmail.com, and https://m.youtube.com. You can sometimes find a link for the mobile or basic HTML version of a Web site among the small links toward the bottom of the site's main page.

1.2 Security Risks with Web Proxies:

You should be aware of some of the risks associated with the use of Web proxies, particularly those operated by individuals or organizations you do not know. If you use a Web proxy simply to read a public Web site such as www.bbc.co.uk, your only real concerns are that:

- Someone might learn that you are viewing a censored news source.
- Someone might learn which proxy you rely on to do so.

Furthermore, if your Web proxy is working properly, and if you access it through HTTPS, the former information should only be available to the administrator of the proxy itself. However, if you rely on an insecure HTTP connection or if your proxy malfunctions (or is poorly designed) this information will be revealed to anyone who might be monitoring your Internet connection. In fact, unencrypted Web proxies do not work at all in some countries, because they cannot circumvent filters that rely on keywords, rather than URLs or IP addresses, to block content.

For some users, the risks above are not a major concern. However, they may become quite serious if you intend to use a Web proxy to access certain types of online resources, such as:

- sites that require you to log in with a password
- sites through which you intend to access sensitive information
- sites through which you intend to create or share content
- online commerce or Web banking sites
- sites that support HTTPS encryption themselves.

In such cases, you should avoid using insecure or un trusted Web proxies. In fact, you might want to avoid using a Web proxy altogether. While there is no guarantee that a more "advanced" tool will be more secure, the challenges that installable circumvention software must address in order to keep your traffic private are generally less complex than those faced by Web proxy software.

1.3 Obfuscation is not Encryption:
Some Web proxies, most notably those that lack support for HTTPS, use simple encoding schemes to circumvent poorly-configured domain name and keyword filters. One such scheme, called ROT-13, replaces each character with whatever lies 13 places ahead of it in the standard Latin alphabet. (See http://www.rot13.com to try it out for yourself.) Using ROT-13, the URL http://www.bbc.co.uk becomes uggc://jjj.oop.pb.hx, which would make it unrecognizable to a very basic keyword filter. Proxy designers have found this trick useful even in countries where keyword filtering is not present, because Web proxies often include the target URL inside the actual URL that your browser sends to the proxy every time you click on a link or submit a new address. In other words, when using a proxy, your browser might request http://www.proxy.org/get?site=http://www.bbc.co.uk instead of just http://www.bbc.co.uk, but a domain name filter written to catch the latter would catch the former just as readily. http://www.proxy.org/get?site=uggc://jjj.oop.pb.hx, on the other hand, might slip through the filter. Unfortunately, character encoding schemes are not very reliable. After all, there is nothing to prevent a censor from adding "jjj.oop.pb.hx" to the blacklist along with "www.bbc.co.uk." (Or, better yet, she could add "uggc://" to the list, which would block all use of the proxy.)

The important thing to remember about character encoding is that it does not protect your anonymity from third party observers, who can still track the list of sites that you visit. And, even if it is applied to the full text of the pages you view and content you submit (rather than just to URLs), it still cannot provide confidentiality. If these things matter to you, restrict your use of Web proxies to those that support HTTPS.

Don't forget, the proxy administrator can see everything.

The advice above emphasizes the importance of HTTPS, both on the censored target site and on the proxy itself, when using a Web proxy to create or obtain sensitive information. However, it is important to note that even when you access a secure site through a secure proxy, you are still putting a great deal of faith in whoever administers your Web proxy, as that individual or organization can read all of the traffic that you send or receive. This includes any passwords that you might have to submit in order to access the destination Web site.

Even the more advanced circumvention tools, which tend to require that you install software on your computer, must rely on some kind of intermediary proxy in order to circumvent Web filters. However, all reputable tools of this kind are implemented in such a way as to protect the content of HTTPS Web traffic even from the circumvention services themselves. Unfortunately, this is not possible for Web proxies, which must rely more heavily on good old-fashioned trust. And trust is a complicated function, that depends not only on a service administrator's willingness to protect your interests, but also on her logging and record-keeping policies, her technical competency, and the legal and regulatory environment in which she operates.

1.4 Anonymity Risks with Web Proxies:
Tools designed to circumvent filtering do not necessarily provide anonymity, even those that might include words like "anonymizer" in their names! In general, anonymity is a much more elusive security property than basic confidentiality (preventing eavesdroppers from viewing the information that you exchange with a Web site). And, as discussed above, even to ensure basic confidentiality through a Web proxy requires, at the very least, that you:

- use an HTTPS Web proxy
- connect through that proxy to an HTTPS destination Web site
- trust the proxy administrator's intentions, policies, software and technical competence
- heed any browser warnings, as discussed in the HTTPS chapter of this book.

All of these conditions are also prerequisites for any degree of anonymity. If a third party can read the content of your traffic, he can easily connect your IP address with the list of specific Web sites that you visit. This is true even if, for example, you log in to those sites or post messages on them using a pseudonym. (Of course, the opposite is true, as well. Even a perfectly secure proxy cannot protect your identity if you sign your name to a public post on the destination Web site!)

1.5 Advertising, Viruses and Malware:
Some of the people who set up Web proxies do it to make money. They may do this simply and openly by selling advertisements on each proxied page, as in the example below.

Or, a malicious proxy administrator might try to infect his users' computers with malware. These so-called "drive-by-downloads" can hijack your computer for spamming or other commercial or even illegal purposes.

The most important thing you can do to protect yourself against viruses and other malware is to keep all of your software – especially your operating system and your anti-virus scanner – updated. You can also block ads by using the Ad Block Plus extension (http://www.adblockplus.org) and some malicious content by using the No Script extension (http://noscript.net). Both of these extensions are for the Firefox Web browser. (http://www.stopbadware.org).

1.6 Cookies and Scripts:
There are also risks associated with the use of cookies and embedded scripts. Many Web proxies can be configured to remove cookies and scripts, but many sites (for example, social networking sites like Facebook and media streaming sites like YouTube) require them to work properly. Web sites and advertisers can use these mechanisms to track you, even when you use proxies, and to produce evidence that, for example, the person who did one thing openly is the same person who did another thing anonymously. Some cookies may be saved on your computer even after you restart it, so it might be a good idea to allow only selective use of cookies. In Firefox, for example, you can instruct the browser to accept cookies only "Until I close Firefox".

(Similarly, you can instruct your browser to erase your browsing history when you close it.) Generally speaking, however, Web proxies are extremely limited in their ability to protect your identity from the Web sites that you access through them. If this is your goal, then you will have to be very careful how you configure your browser and proxy settings, and you might want to use a more advanced circumvention tool.

2. VPN OR VIRTUAL PRIVATE NETWORK:
Virtual Private Networks create an encrypted 'tunnel' between your computer and the host server, with the internet traffic going in and out of the host server. Your ISP or government can only see that you have connected to the VPN server and nothing else – your activities, IP addresses you have visited etc. are all completely hidden from them behind a minimum of 128-bit encryption.

2.1 Security Issues:
One of the advantages of using a VPN is that it allows remote users to securely access the enterprise's systems. Unfortunately, this also makes the network susceptible to security breaches. Often, a remote user will use unsecured assets, such as a personal laptop, to access the enterprise's network. If this device has a virus or some other malicious software, it can compromise the network once the user has authenticated his access request and successfully logged on to the servers.
This form of network security threat is difficult for network administrators to manage, because there is a need to rely on the responsibility of the users to ensure that the network remains secure. This is challenging to do because the network access device is not under physical control of the network administrator. Whether or not an employee is given a device to be used exclusively for the company's business, there can be no guarantee that the employee will do so.

2.2 Performance Issues:
Leased lines or a dedicated data services can give an organization guaranteed bandwidth regardless of the traffic load on the network or the requirements of competing entities. In contrast, there can be no bandwidth guarantee on public networks unless elaborate resource sharing protocols such as MPLS are used. Ironically, the use of these protocols, in VPN solutions, tend to knock off a few performance points from the data connection's bandwidth.

Though a properly installed VPN can prevent some of the performance issues associated with supporting multiple protocols and data transmission mediums, VPNs are only as fast as the slowest Internet connection between the two endpoints. In addition, most IP applications were designed for low-latency and high reliability network environments. This means that network performance issues will become more pronounced with the increasing use of real-time and interactive applications. While some applications can be reprogrammed or reconfigured to work with increased latency, getting this workaround to work with some applications can be challenging, if not impossible.

Similarly, it might be difficult to get VPN solutions from different providers to work with each other due to the different standards and protocols that may be in use. This should become less of an issue as service providers adopt more generally accepted standards and the industry becomes more mature.

2.3 Complexity:
VPNs often use multiple network topologies, protocols, network hardware equipment and service providers to establish a single VPN tunnel. Using several data services providers can make a network more robust, but at the same time, trying to get several network components to work well together can only create complexity, especially if most of these components weren't designed to work together.

In order to get a VPN to work well, an enterprise might need to employ additional network specialists to configure and administrate the network or acquire additional equipment; all of which may make the VPN solution more costly to implement and maintain.

3. CONCLUSIONS:

VPN is superior in almost every way to proxies. It provides vastly improved online anonymity, and protects your entire on-line life. In addition to this, because ISPs cannot monitor your online activity, it is an effective means of bypassing ISP throttling.

The only reason for choosing a proxy service over VPN is price.

Base	Proxy	VPN
Online Security	It gives very low-level security. Only on SSL connection everything is encrypted but on non-SSL connection everything is vulnerable to cyber threats.	It gives high-level encryption up to 256-bit. VPN is more like a safe vault, once you have availed it, all your communications are completely secure.
Online Privacy	When using a Proxy, anyone can intercept your private data.	With VPN all your data is totally encrypted and therefore no one can intrude in your privacy, not even your ISP can monitor your activities.
Online Freedom	It only works for certain geo-restrictions and cannot help you bypass strong firewalls and censorship.	With VPN, you can access any website from anywhere in the world.
Speed	It does compromise your internet speed to great extent due to overloaded servers.	With VPN, you can avail best solutions to boost up your internet speed such as Smart DNS. VPN doesn't compromise your internet speed.
Compatibility	It is limited only to certain browsers.	It works with all OS and devices such as Windows, Android, iOS, Linux, Mac and Routers.
Reliability	Only works for bypassing geo-restricted channels and provides no security at all. Hence, not reliable.	It is the most sophisticated tool to ensure your online security, privacy and freedom at same time. Hence, 100% reliable.
Stability	It usually crashes most of the time. It gives maximum downtime, even when you are in the middle of downloading or streaming.	VPN is 99.9% stable and provides you maximum up-time.

REFERENCES:

1. "Tor developers vow to fix bug that can uncloak users". http://arstechnica.com/security/2014/07/tor-developers-vow-to-fix-bug-that-can-uncloak-users/
2. "Free Haven's Selected Papers in Anonymity". http://freehaven.net/anonbib/#2014
3. "TorResearchHome". https://research.torproject.org/
4. http://www.pcworld.com/article/2686467/how-to-use-the-tor-browser-to-surf-the-web-anonymously.html
5. http://software.sonicwall.com/applications/app/index.asp?ev=appd&appid=1732&app_name=GAppProxy
6. http://freenuts.com/how-to-install-and-use-gappproxy/
7. http://freenuts.com/how-to-install-and-use-hyk-proxy/
8. https://docs.google.com/document/d/1fROW15y2nO8LoE3heU7slgE6lAsWerA-K4vCc4DGfqKE/pub#h.6qijc2ytnh0h
9. http://gpass.software.informer.com/
10. http://freenuts.com/free-proxy-softwares/
11. http://bitvise-tunnelier.software.informer.com/
12. https://www.bitvise.com/ssh-server-guide-installing
13. https://psiphon3.com/en/index.html
14. https://psiphon3.com/en/user-guide.html
15. https://www.proxpn.com/index.php#more-features
16. https://www.proxpn.com/index.php#more-how
17. https://www.securitykiss.com/faq/
18. https://www.securitykiss.com/resources/tutorials/how_to/
19. https://www.hotspotshield.com/
20. https://www.hotspotshield.com/benefits-of-vpn/
21. https://www.hotspotshield.com/lp/pages/support.html
22. https://nordvpn.com/fr/about-us/
    http://www.kabatology.com/11/24/how-to-setup-open-source-ultravpn-in-ubuntu/
23. http://freevpn.org/
24. https://support.cyberghostvpn.com/index.php?/Knowledgebase/Article/View/260/0/how-to-use-cyberghost-vpn
25. https://airvpn.org/aboutus/
26. http://www.vpnsp.com/vpnod.html
27. https://openvpn.net/index.php/about-menu/about-us.html